KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer – Simple yet Effective

Raccoon Stealer aka 'Racealer' or 'Mohazo', first circulated around mid 2019 is back after the temporary shutdown in March 2022 following the death of one of the malware authors during Ukraine's invasion by Russia. Embracing their Malware-as-a-Service (MaaS) model, the threat group is promoting the C/C++ written Raccoon Stealer 2.0 with improved capabilities along with a beta program, dedicated technical support team and bug fixes & updates. The subscription also offers an admin login panel to threat actors to be customize, access stolen data and new builds of the stealer.

Often distributed, via exploit kits, phishing campaigns and Potentially Unwanted Applications (PUAs), Raccoon stealer targets both 32- & 64-bit windows machines using just 8 legitimate DLLs. The malware comes with hardcoded RC4 encrypted & base 64 encoded private keys to connect to C2 which further communicates the specific configuration and other C2 URLs hosting the DLLs. The malware targets roughly 60 applications for sensitive data like browsing data (cookies, history, and autofill), credentials, credit card information and crypto wallets along with screenshots and access to files in disk. It is also shipped with a dropper feature which could be configured to download and launch any second-stage malware appealing to wider cybercriminals. Raccoon uses '%Temp%' as its working folder and compresses all stolen data into a single zip file to exfiltrate to C2 via a plain HTTP Post method without any encryption & deletes itself.

Contrary to most malware, Raccoon isn't equipped with advanced defense evasion techniques such as anti-analysis, obfuscation or disabling defenses. It's simple yet effective approach coupled with low entry barrier has made it a popular among cybercriminals and has been observed to increasingly affect systems around the world.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer – Simple yet Effective

Indicators of Compromise: IP Addresses	
104.21.66[.]99	87.120.254[.]71
45.89.54[.]140	167.172.35[.]218
77.75.230[.]25	94.158.244[.]114
93.115.28[.]51	88.119.170[.]241
85.192.63[.]46	35.189.105[.]242
34.90.238[.]61	35.198.183[.]218
34.77.205[.]80	51.195.166[.]185
31.31.198[.]12	194.180.174[.]95
5.182.36[.]154	185.225.19[.]229
77.75.230[.]39	172.67.157[.]163
89.208.104[.]46	213.252.247[.]97
146.70.125[.]95	172.67.169[.]213
194.76.226[.]22	176.124.212[.]169
34.89.185[.]248	194.180.174[.]118
34.77.164[.]226	194.180.174[.]104
194.87.94[.]240	185.163.204[.]216
206.189.100[.]203	

Indicators of Compromise: Domains	
isns[.]net	krupskaya[.]com
majul[.]com	njxyro.ddns[.]net
inexu[.]top	p3.adhitzads[.]com
majul[.]com	frederikkempe[.]com
telegka[.]top	m-onetrading-jp[.]com
telegatt[.]top	searchkn1.sima-land[.]ru
epifile[.]info	vcctggqm3t.dattolocal[.]net
filetick[.]pro	booking.msg.bluhotels[.]com
qxq.ddns[.]net	tracker.internetwarriors[.]net
192-168-100-240.otmn.direct.quickconnect[.]to	
device-local-3193b8ff-0889-41c5-8fd6-67066f88b277[.]remotewd.com	

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer – Simple yet Effective

Indicators of Compromise: Hashes
0cfa58846e43dd67b6d9f29e97f6c53e
16bae91061e6410ddf2c17b544939d87
214add3ebdd5b429fda7c00e7f01b864
59c9737264c0b3209d9193b8ded6c127
88a354d8d051d4dd8c741cdf3e986244
b35cde0ed02bf71f1a87721d09746f7b
c5ce68e5feabffe94ce4309e9e278a91
eca370e62443218965eb27b1a61bb7a0
51c33c00a3823180a7b39ab838542d9d
7a1618c1616dae2aa4402b2f9f0febc7
1de2a5e94f070e9d6e8d70fe63e87175
c8f9b86af75c8cb9f973683dbee27f93
704cb6b7d8863165857bca2c33283fa0
e490eacd7d52073891790cd3411a1221
52b4394897b2ddd3c47ec410ea1ff869
2eb2d4dc60b185e1961746b120d45f97
ecc322f22da7cee63fb2ee0bfd5df59c
0cf266265f77e387a9d396888651240f2b458e0a
4436a1c572737a82494d4ddfe91929ce4cd836cd
465d756d89a18d40a2721e74d99b4df8dc9438a8
48ca383575fdc914ed3436d40201eae6bac55007
4e48d0c38e0a4543137cd381abb38e6bd17f17aa
9c6e393d8b2eac432720518f8991c86ad8fa94b7
ab272e68f0e09391e3675cf8cda344774ae98769
abe82a1405471258c72d031191846ea627f1c63c
b47cc17316ef37a18919eedd0ec16908febac7a1
b997c212dee402190a4fe7562fa68f565c084711
2ccd8f8985421013be97e828b5a355904369e2e3
825461b7b608440629265de07860183ef4e923ca
a19176e040857c11ea94f2b68dd3dcdd1c284d44
1b24c8e90661994259f4698b6996ceaa62c9e31a
9885624e1d99a38e09e074224f96a3bb3d5f5039
be6e702b0200e41d8222dcfdc7c8a40837798011
cf376cf7b2b058a2502a8e0374c71cc6c1c32eba

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer – Simple yet Effective

Indicators of Compromise: Hashes
772b54a26db6e20714930432b7fec95069c0d4e4
1ab3990c0182facec052f9c2121c77509e48ab25
e31b9ebbd14d64dc00cb92c77120d71e718728b9
c791b860197865abce4e4d3c1c1dece67946c458
fa0687a0f923a3a937abb96c5f634b580997648e
e588c7a3718437d5c70e72e4b095398360740506
eac3400bc97097b5d9cb68313d733c679c959109
a378d72233a18ea0c96706e04982db80fc67ce1a
5b47f1a54e2e50cd9dfdcd475430a0f21e179560
32d8b327c5a3c4b62c9af796bd57bb5414305446
a9d4da96cf6210cb3138c2f22f2445b95ed57086
f2de92e3c7455d2989d3fca19ac2d62f1e4c43f4
cb1d307fe843842f7f777642959e9a0214eb5c3e
addfc32f5b3497201dbd7673fde77004ecb41551
d282c0f49a6ef8c4ba96f3144d935646bb1acac3
46e19fa43ffca2f91b9e77c9652f8592e76fd07c
6b0acdaff000ac56e37c344f47119e520febb703
8acdbd56820d73c2fa29b5a3613c4539732b7557
672ba829a128d2d10bd174525ed1d56d16f83a0e
11c2d0d8ed73b5e45ceb59f5c109ee7f52b0e1c7
290aa47a0ef23859ad49cef908b53b5eb303d4bc
c212c36dc980106c8eac3796d77afd31e08e0025
2c9f1938c85c697d877de78573424c45bbc27728
9d9331cc8ea734d526020ec9dca692972816dbcf
cd7279865f441b7decbd75f764fef4b44136f5d2
d056310e01c513a7d47307c3427ddecb1b0b4c34
af9c488a79477b478f1992d1dec17dc934902c9f
b88b6a5666e874e4a1a7c739826521803129397a
bf89795daa7ba6705c33e2f5ed2b4a0cafe8f0b2
20d82cf37b710a2d4e74730b8cab7e4a9b578209
883f8ea706650fe0dde587d701fa822e1aaa1813
85341e754f56c95c58416ba1b2c010544cfb0b0f
d1bbff45f7090de973ec7c213546e2d3e64a37e4
310ea0165e41c6f303f297c883f2cebd16f09ea6

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer – Simple yet Effective

Indicators of Compromise: Hashes
a12d16f62c9e38633699b8f5e88a153b9fb8f02b
639b8a2a714ba900c65871eb08006dce42da0a9b
d66c9f4a24ebf01ba18bcdff9e5fc2c4b517cbb4
b7d4a9725cdee35a7b88ce1b9bca9071e0c25035
69623f12a9f7113a6dbf4e2ae8b38ea1f9c7a41f
fa430e10178776a028babb37d63a4b132c7c51ce
f912a64f5de145f65a289c3f215222dc4bb79323
1138339d89a58121533d6d299a8b3a2f71ece4ee
1b8106efdda6723c9c75601518d094ed5c867c39
4a36335445f0a3395c397939bd358b1bb0f50e28
0c77ec36379ffd5c9b66c12d1622ad5807eb46f4
5ccdb96521b465db0576ac3136ec8a8ff2d124c2
022432f770bf0e7c5260100fcde2ec7c49f68716751fd7d8b9e113bf06167e03
0c722728ca1a996bbb83455332fa27018158cef21ad35dc057191a0353960256
2106b6f94cebb55b1d55eb4b91fa83aef051c8866c54bb75ea4fd304711c4dfc
263c18c86071d085c69f2096460c6b418ae414d3ea92c0c2e75ef7cb47bbe693
47f3c8bf3329c2ef862cf12567849555b17b930c8d7c0d571f4e112dae1453b1
62049575053b432e93b176da7afcbe49387111b3a3d927b06c5b251ea82e5975
7299026b22e61b0f9765eb63e42253f7e5d6ec4657008ea60aad220bbc7e2269
7322fbc16e20a7ef2a3188638014a053c6948d9e34ecd42cb9771bdcd0f82db0
9ee50e94a731872a74f47780317850ae2b9fae9d6c53a957ed7187173feb4f42
a57e1f3217b993476c594570095d28b6c287731a005325e5f64a332a86cb7878
bd8c1068561d366831e5712c2d58aecb21e2dbc2ae7c76102da6b00ea15e259e
c6e669806594be6ab9b46434f196a61418484ba1eda3496789840bec0dff119a
F7b1aaae018d5287444990606fc43a0f2deb4ac0c7b2712cc28331781d43ae27